REMARKS

Claims 1-11 are active.

Claims 1-11 stand rejected over Sedlak, U.S. 4,870,681. Claims 2-10 depend from main method claim 1, and claim 11 is an apparatus claim.

Method claim 1 and apparatus claim 11 have been amended to set forth that the number for l is equal to or larger than 2. This amendment is supported at page 14, line 13 where the case l equal to 2 is specifically discussed. Furthermore, reference is made to page 15, lines 4 and 34, line 16, lines 14 and 15 which shows the case l equal to 3. Reference is also made to page 16, lines 28-32, where the case l equal to 2, l equal to 3, l equal to 4 and higher integers for l are mentioned.

Sedlak does not disclose the step of or apparatus for l to be equal to 2 or greater, as set forth in claims 1 and 11 as determined for any of:

1. the multiplication shift values. Instead, Sedlak only determined a single multiplication shift value.

2. the at least two multiplication shift values, in which at least two blocks of consecutive digits of the multiplier are taken into account. Instead, in Sedlak only a single block of consecutive digits for determining a single multiplication shift value is used.

3. the reduction shift values. Instead, he only discloses to determine a single reduction shift value.

Sedlak also does not disclose the claimed step of or apparatus for applying so as to obtain 2l+1 operands, i.e., at least five operations, when l is equal to 2. Instead, Sedlak teaches performance of a 3-operand addition as shown in Fig. 6(b), the sixth box from the bottom.

Finally, Sedlak also does not disclose the claimed step of or apparatus for combining the operands, since it does not disclose to calculate at least five operands.

Thus, Sedlak does not anticipate the subject matter of the present invention as defined in amended claims 1 and 11.

For accelerating multiplication using the Sedlak algorithm, those skilled in the art would have several possibilities. The first possibility, which is very straight forward, would be to use a faster processor. A further possibility would be to replace the single processor principle as defined in Sedlak, and as shown by the flow charts in Figs. 5 and 6, by a processor having parallel single processors. The question is, however, how these parallel single processors can work. Possibly, the functionality of the block GEN_Mult_LA could be performed in parallel to the functionality of the block GEN_Mod_LA. This would mean that the multiplication look-ahead-algorithm is operated in parallel to the reduction look-ahead algorithm.

A completely different solution is, however, accomplished by the present invention.

That is, the subject application is directed to a novel method and apparatus for performing a mixed parallelization with respect to the determination of the multiplication shift values and the reduction shift values. To this end, several blocks of digits of the multiplier are processed to determine the shift values, with this preferably performed in parallel. In the step of and apparatus for applying, however, the intermediate result from the preceding iteration alteration step is used for generating the $2l+1$ operands, so that the serial nature for generating one intermediate result after the other (or by performing one iteration step after the other) is maintained.

The latter emphasizes that the step of and apparatus for applying the l multiplication shift values and the l reduction shift values cannot be performed in any way but has to be performed so that $2l+1$ operands result. For l equal to 2, exactly five operands result. For l equal to 3, exactly seven operands result. For l equal to 4, exactly 9 operands result, etc.

Then, in order to complete the current iteration step, the operands obtained by the step of and apparatus for applying are combined to calculate a new updated

intermediate result. In accordance with the present invention, the updated intermediate result is an intermediate result, which is obtained by a single iteration step. In accordance with Sedlak, one would need several iteration steps to obtain the same intermediate result. Therefore, applicant's invention results in a more efficient method and apparatus.

Accordingly, it is clear that main method claim 1 and apparatus claim 11 respectively define a novel method and apparatus for performing a modular multiplication of a multiplicand and a multiplier for a data processing means. Therefore, these claims are patentable and should be allowed.
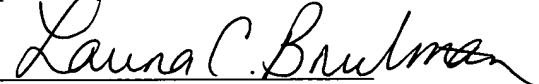
Claims 2-10 depend directly on allowable claim 1 and recite further novel features of the invention. Accordingly, these claims also should be allowable.

The other art cited has been considered and is not deemed pertinent.

Prompt and favorable action is requested.

Dated: September 9, 2005   Respectfully submitted,

By _Laura C. Brutman_
Laura C. Brutman
    Registration No.: 38,395
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(206) 262-8900
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant